IN THE CLAIMS

1. (Currently Amended) A method for establishing secured roaming among a wireless station, a first and a second access points, comprising:

the first access point requesting a first ticket from an authentication server and using the first ticket to establish a first secured session between the first access point and ~~with~~ the wireless station; and

in response to a second ticket request from the wireless station through the first secured session, the first access point forwarding the second ticket request to the authentication server and relaying a resulting second ticket from the authentication server to the wireless station, the second ticket being different than the first ticket, wherein the second ticket is used to establish a second secured session between the wireless station and the second access point.

2. (Previously Presented) The method according to claim 1, the method further comprises:

applying the second ticket and a group identity shared by the first and the second access points to establish a second secured session between the wireless station and the second access point, the group identity identifying that the first and second access points belong to the same group, and wherein the wireless station can only access another access point within the same group identified by the group identity using the second ticket.

3. (Previously presented) The method according to claim 1, the method further comprises:

the authentication server dynamically generating a first and a second session keys to include in the first and the second tickets, respectively; and

the authentication server encrypting the first and the second tickets with a first and a second encryption keys.

4. (Original) The method according to claim 3, the first and the second session keys have limited lifetime.

5. (Previously presented) The method according to claim 3, the method further comprises:

the first access point appending application specific information to the second ticket to formulate a combined message; and

the first access point encrypting the combined message with the first session key.

6. (Original) The method according to claim 5, the application specific information further comprises the first access point's selected time and random number.

7. (Previously Presented) An access point in a secured wireless roaming system, comprising:

an antenna;

a filter coupled to the antenna;

a receiver and a transmitter coupled to the filter; and

a control unit coupled to the receiver and the transmitter and coupled to a wired-network connection interface, wherein the control unit further comprises an authentication protocol engine that

requests a first ticket from an authentication server and uses the first ticket to establish a first secured session with a wireless station; and

in response to a second ticket request from the wireless station through the first secured session, forwards the second ticket request to the authentication server and relays a resulting second ticket from the authentication server to the wireless station, the second ticket being different than the first ticket, wherein the second ticket is used to establish a second secured session between the wireless station and the second access point.

8. (Original) The access point according to claim 7, the control unit further comprises:

an encryption/decryption engine to decrypt the second ticket request before the authentication protocol engine forwards the second ticket request.

9. (Previously Presented) The access point according to claim 7, wherein the authentication server further:

dynamically generates a first and a second session keys to include in the first and the second tickets, respectively; and

encrypts the first and the second tickets with a first and a second encryption keys.

10. (Original) The access point according to claim 9, the first and the second session keys have limited lifetime.

11. (Previously Presented) The access point according to claim 8, further comprises:

the authentication protocol engine to append application specific information to the second ticket to formulate a combined message; and

the encryption/decryption engine to encrypt the combined message with the first session key.

12. (Original) The access point according to claim 11, the application specific information further comprises the access point's selected time and random number.

13. (Previously Presented) A wireless station in a secured wireless roaming system, comprising:

an antenna;

a filter coupled to the antenna;

a receiver and a transmitter coupled to the filter; and

a control unit coupled to the receiver and the transmitter, wherein the control unit further comprises an authentication protocol engine that

requests a second ticket from an authentication server via a first secured session established with a first access point using a first ticket, the second ticket being different than the first ticket, and

establishes a second secure session with a second access point using the second ticket received via the first secured session.

14. (Previously Presented) The wireless station according to claim 13, comprising:

the authentication protocol engine to apply the second ticket and a group identity shared by the first and the second access points to establish a second secured session with the second access point, the group identity identifying that the first and second access points belong to the same group, and wherein the wireless station can only access another access point within the same group identified by the group identity using the second ticket.

15. (Previously Presented) A secured wireless roaming system, comprising:

a wired medium;

a wireless medium;

an authentication server coupled to the wired medium;

a wireless station coupled to the wireless medium; and

an access point coupled to the wireless medium and the wired medium, wherein the access point comprises:

a first control unit, comprising a first authentication protocol engine to request a first ticket from the authentication server and use the first ticket to establish a first secured session with the wireless station; and

in response to a second ticket request from the wireless station through the first secured session, to forward the second ticket request to the authentication server

and relays a resulting second ticket from the authentication server to the wireless station, wherein the second ticket is different than the first ticket and the second ticket is used by the wireless station to establish a second secured session with another access point coupled to the wired and wireless mediums.

16. (Previously Presented) The secured wireless roaming system according to claim 15, wherein the wireless station further comprises:

a second authentication protocol engine to apply the second ticket and a group identity shared by the first and a second access points to establish a second secured session with the second access point, the group identity identifying that the first and second access points belong to the same group, and wherein the wireless station can only access another access point within the same group identified by the group identity using the second ticket.

17. (Original) The secured wireless roaming system according to claim 15, the first control unit further comprises:

an encryption/decryption engine to decrypt the second ticket request before the authentication protocol engine forwards the second ticket request.

18. (Previously presented) The secured wireless roaming system according to claim 15, wherein the authentication server further:

dynamically generates a first and a second session keys to include in the first and the second tickets, respectively; and

encrypts the first and the second tickets with a first and a second encryption keys.

19. (Original) The secured wireless roaming system according to claim 17, the first and the second session keys have limited lifetime.

20. (Previously presented) The secured wireless roaming system according to claim 17, further comprising:

the first authentication protocol engine to append application specific information to the second ticket to formulate a combined message; and

the first encryption/decryption engine to encrypt the combined message with the first session key.

21. (Original) The access point according to claim 20, the application specific information further comprises the access point's selected time and random number.

22. (Currently Amended) The method of claim 1, wherein the second ticket is only valid for the second secured session between the ~~wirelessly~~ wireless station and the second access point.

23. (Previously Presented) The method of claim 22, wherein the second ticket is only valid for the second secured session for a predetermined period of time.

24. (Previously Presented) The method of claim 3, wherein the first access point requesting a first ticket from an authentication server comprises:

the wireless station providing an identification (ID) of the wireless station to the first access point;

the first access point obtaining the first ticket from the authentication server; and

the first access point establishing the first secured session using the newly obtained first ticket.

25. (Previously Presented) The method of claim 24, further comprising the wireless station obtaining a group ID from the first access point via the first secured session, the group ID being shared with the first and second access points and identifying that the first and second access point belong to the same group, wherein the wireless station can only access another access point within the same group.

26. (Previously Presented) The method of claim 25, wherein the second secured session is established based on the second session key and the group ID.

27. (Previously Presented) A machine-readable medium having executable code to cause a machine to perform a method for establishing secured roaming among a wireless station, a first and a second access points, the method comprising:

the first access point requesting a first ticket from an authentication server and using the first ticket to establish a first secured session with the wireless station; and

in response to a second ticket request from the wireless station through the first secured session, the first access point forwarding the second ticket request to the authentication server and relaying a resulting second ticket from the authentication server to the wireless station, the second ticket being different than the first ticket, wherein the second ticket is used to establish a second secured session between the wireless station and the second access point.